UNITED STATES DISTRICT COURT

for the
Central District of California

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
31251 Belford Drive, San Juan Capistrano, California 92675

Case No. 8:18-MJ-00545

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

☑ evidence of a crime;

☑ contraband, fruits of crime, or other items illegally possessed;

☑ property designed for use, intended for use, or used in committing a crime;

☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 2251(d), 2252A(a)(2), (a)(5)(B)	See attached affidavit

The application is based on these facts:

See attached Affidavit

☑ Continued on the attached sheet.

☐ Delayed notice of ______ days (give exact ending date if more than 30 days: ____________) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

____
Applicant's signature

Kevin Leduc, Special Agent, HSI
Printed name and title

Sworn to before me and signed in my presence.

Date: ____________

____
Judge's signature

City and state: Santa Ana, California

Douglas F. McCormick, U.S. Magistrate Judge
Printed name and title

AUSA: Jake Nare, 714-338-3549

AFFIDAVIT

I, Kevin Leduc, being duly sworn, declare and state as follows:

I. **INTRODUCTION**

1. I have been employed as a Special Agent (“SA”) of the U.S. Department of Homeland Security, Homeland Security Investigations (“HSI”) since 2017, and I am currently assigned to the Child Exploitation Investigations Group in Orange County. Prior to my employment as a Special Agent, I was employed as a Computer Forensic Analyst with HSI from 2014-2017. My responsibilities as a SA include investigating crimes involving the sexual exploitation of minors, including, but not limited to, offenses involving travel in foreign commerce to engage in sexually explicit conduct with minors, and offenses involving the production, possession, and transportation of child pornography.

2. I have completed the Criminal Investigator Training Program and Immigration and Customs Enforcement Special Agent Training at the Federal Law Enforcement Training Center in Brunswick, Georgia. I have also received specific training in the investigation of child exploitation offenses, and I have conducted and participated in numerous child exploitation investigations. As part of these investigations, I have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. Moreover, I am a federal law enforcement

officer who is engaged in enforcing criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

II. PURPOSE OF AFFIDAVIT

3. This affidavit is made in support of an application for a warrant to search the premises located at 31251 Belford Drive, San Juan Capistrano, California 92675 (the “SUBJECT PREMISES”), more fully described below and in Attachment A, which is attached hereto and incorporated herein by reference, and to seize evidence, fruits, and instrumentalities of criminal conduct, as specified in Attachment B, which is also attached hereto and incorporated by reference, of violations of 18 U.S.C. §§ 2251(d)(advertisement of child pornography), 2252A(a)(2) (receipt and distribution of child pornography), and 2252A(a)(5)(B) (possession of child pornography) (collectively, the “Subject Offenses”).

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

III. **PREMISES TO BE SEARCHED**

5. The SUBJECT PREMISES, as described in this paragraph and in Attachment A, is the property located at 31251 Belford Drive, San Juan Capistrano, CA 92675. The SUBJECT PREMISES is located on the southeast side of Belford Dr. The SUBJECT PREMISES is a two-story family residence with an attached three car garage, one white double garage door and one single white garage door both facing northwest. The SUBJECT PREMISES has a light green wood paneling façade with white trim and a gray shingle roof. The front door of the SUBJECT PREMISES is Northwest facing. The numbers “31251” are affixed in black numbers on the white trim of the house facing the street.

IV. **SUMMARY OF PROBABLE CAUSE**

6. Along with other members of law enforcement, I have been investigating individuals who are trading child pornography on the Internet through peer-to-peer file-sharing programs. As set forth in greater detail below, law enforcement has identified a computer making child pornography files available for sharing on the Gnutella network, which is described in detail below, between August 02, 2018 and August 14, 2018. On each occasion, that computer was connected to the Internet using Internet Protocol (“IP”) address 68.5.130.12 (“SUSPECT IP ADDRESS”). Law enforcement successfully downloaded approximately sixteen suspected child pornography partial files from this computer, while it was using the SUSPECT IP ADDRESS. The partial files when played clearly contain child exploitation

material. The SUSPECT IP ADDRESS resolves to an Internet subscriber at the SUBJECT PREMISES.

7. On September 14, 2018 Cox Communications returned a DHS Summons confirming that the SUSPECT IP ADDRESS was registered to Rick Brandelli at 31251 Belford Drive, San Juan Capistrano, California 92675. A registered sex offender named Daniel Brandelli ("Brandelli") currently resides at the above-mentioned address. Brandelli was previously the subject of an HSI child exploitation investigation in 2013.

8. Thus, and as set forth more fully below, there is probable cause to believe that the SUBJECT PREMISES contains evidence of the Subject Offenses.

V. **DEFINITION OF TERMS**

9. The following terms have the indicated meaning in this affidavit:

a. The terms "minor," "sexually explicit conduct," "visual depiction," "producing," and "child pornography" are defined as set forth in 18 U.S.C. § 2256.

b. The term "computer" is defined as set forth in 18 U.S.C. § 1030(e)(1).

c. The term "Internet" is defined as the worldwide network of computers — a noncommercial, self-governing network devoted mostly to communication and research with roughly 3.2 billion users worldwide. The Internet is not an online service and has no real central hub. It is a collection of tens of thousands of computer networks, online services, and single user components. In order to access the Internet, an individual computer user must use an access provider, such as a university, employer, or commercial Internet Service Provider (“ISP”), which operates a host computer with direct access to the Internet.

d. The term “Internet Protocol” (“IP”) is defined as the primary protocol upon which the Internet is based. IP allows a packet of information to travel through multiple networks (groups of linked computers) on the way to its ultimate destination.

e. The term “IP Address” is defined as a unique number assigned to each computer directly connected to the Internet (for example, 74.100.66.74). Each computer connected to the Internet is assigned a unique IP address while it is connected. The IP address for a user may be relatively static, meaning it is assigned to the same subscriber for long periods of time, or dynamic, meaning that the IP address is only assigned for the duration of that online session.

f. The term “Internet Service Provider” (“ISP”) is defined as a business that allows a user to dial into or link through its computers, thereby allowing the user to connect to the Internet for a fee. ISPs generally provide only an Internet connection, an electronic mail address, and maybe Internet browsing software. A user can also connect to the Internet through a commercial online service such as AT&T, Verizon, or Time Warner Cable. With this kind of connection, the user gets

Internet access and the proprietary features offered by the online service, such as chat rooms and searchable databases.

g. The term “peer-to-peer” (sometimes referred to as “P2P”) has come to describe applications or programs that allow users to exchange files with each other directly or through a mediating server via the Internet.[1] A decentralized peer-to-peer file transfer network does not follow a model using different clients or servers; rather, it is a network of equal peer computers that simultaneously function as both “clients” and “servers” to the other users on the same network.

h. The term “open source” is defined as software that includes a free license; in other words, it is freely available to everyone using the Internet.

i. The term “share folder,” in the context of peer-to-peer software, is a folder or directory on a computer’s hard drive, which a peer-to-peer user can set up to share his/her contents with other computers on a peer-to-peer network.

j. The term “browsing” is used in reference to P2P networks and refers to the ability of a peer-to-peer user to look at or browse the shared files of another peer-to-peer user.

k. The terms “jpeg,” “jpg,” “gif,” “bmp,” and “art” are defined as graphic image files, namely, pictures.

[1] A computer that is performing tasks for other computers that are connected to it is often called a “server.” A “client” computer is one that is connected to a server and is making requests of the server.

l. The terms “mpeg,” “mpg,” “mov,” “avi,” “rm,” and “wmv” are defined as video or movie files. To use these video files, one needs a personal computer or other digital device with sufficient processor speed, internal memory, and hard disk space to handle and play typically large video files. One also needs a video file viewer or client software that plays video files. One can download shareware or commercial video players from numerous sites on the Internet.

m. The term virtual private network (“VPN”) is defined as a method of sending all of an Internet user’s Internet traffic through a private, encrypted tunnel. The use of a VPN provides greater control of how a user is identified online. A VPN creates a virtual encrypted “tunnel” between an Internet user and a remote server operated by a VPN service. All external Internet traffic is routed through this tunnel, so that the Internet user’s ISP cannot see the data being transmitted. The end result is that the Internet user’s computer appears to have the IP address of the VPN server, masking the true identity of the Internet user. VPN’s are used as a tool to protect the privacy of individuals and businesses, but are also widely used by criminals to disguise their true geographic location in order to evade identification by law enforcement.

VI. BACKGROUND ON USE OF COMPUTERS, CHILD PORNOGRAPHY, AND P2P FILE-SHARING TECHNOLOGY

10. Based upon my training, experience, and knowledge gained from speaking with other knowledgeable officers, agents, and investigators in the investigation of child pornography and with P2P file-sharing programs, and information related to me by other law enforcement officers involved in the investigation of child pornography generally, I know the following information about the use of computers with child pornography.

11. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. Child pornographers can now produce both still and moving images directly from a common video camera and can scan these images into computer-readable formats. The use of digital technology has enabled child pornographers to electronically receive, distribute, and possess large numbers of child exploitation images and videos with other Internet users worldwide.

12. Peer-to-peer networks are frequently used in the trading of child pornography. I know that one such network is known as the Gnutella network. The Gnutella network is being used to trade digital files, including still images and movie files, of child pornography. Based on my training and experience, I know the following about the operation of the Gnutella file-sharing network:

a. Gnutella is an open-source publicly available peer-to-peer file-sharing network. Most computers that are part of this network are referred to as peers or hosts. A peer computer can simultaneously share files, while downloading files from other peers. Peers may be elevated to temporary indexing servers referred to as an “ultra-peer.”

b. Ultra-peers increase the efficiency of the Gnutella network by maintaining an index of the file contents of network peers. Gnutella users ask ultra-peers for file sources and are directed to one or more peers sharing the file or portions of the file. There are many ultra-peers on the network.

c. The Gnutella network can be accessed by computers running different peer-to-peer software programs written to be used on the Gnutella network. These software programs are known as client programs. Some of the free publicly available software clients are Limewire, BearShare, Phex, and Shareaza. Shareaza is the software program being used in this case. These software programs share common protocols for network access and file sharing. The user interface, features and configuration may vary between the different software clients but all of them allow you to access the Gnutella network as either a client (the computer seeking a file), a candidate (the computer supplying the file), or an ultra-peer (the computer referring the client to the candidate).

d. During the default installation of a Gnutella software program, settings are established that configure the host computer to share files. Based on my training, experience, and knowledge gained from speaking with other knowledgeable agents, officers, and investigators, the level of file sharing and/or number of files to be shared with a single peer can be manipulated in the settings of the Gnutella client software program. A feature known as browsing may also be turned on. Depending upon the Gnutella client program used, a user may have the ability to reconfigure some of these settings during installation or after the installation has been completed. Typically, the peer-to-peer software can be configured to establish the location of one or more directories or folders whose contents (files) are made available for distribution or sharing to other Gnutella peers. Typically, the peer-to-peer software can be configured to establish whether other users of the network can obtain a list or browse the files being shared by the host computer. I know that if an investigator is able to browse a shared directory on a candidate’s computer, a direct connection between the computer being used by the investigator and the candidate’s computer is established at that specific time, on that specific date. I also know that the browsed files are physically present at that time, on that date, on the candidate’s computer.

13. The Internet Crimes Against Children (“ICAC”) Task Force operates under the direction of the Office of Juvenile

Justice and Delinquency Prevention, and in conjunction with the Immigration and Customs Enforcement service ("ICE") (formerly the United States Customs Service), Federal Bureau of Investigation ("FBI"), and the National Center for Missing and Exploited Children ("NCMEC"). The ICAC maintains a list of verified positive child pornography "SHA1 values," explained below.

14. SHA1 or "Secure Hash Algorithm Version 1," is a mathematical encryption method used to produce a unique digital signature of a file. No two files naturally produce the same SHA1 value unless the contents are identical; thus, the content of some computer files can be positively established without ever viewing the content, once a known file with a certain SHA1 value has been identified. SHA1 values were specifically developed by government agencies, including the National Security Agency, to assist in the unique identification of computer files. The United States of America has adopted the SHA1 hash algorithm described herein as a Federal Information Processing Standard. A file processed by this SHA1 operation results in the calculation of a unique hash value for that file, often referred to as a digital signature. SHA1 signatures provide a certainty exceeding 99.99 percent that two or more files with the same SHA1 signature are identical copies of the same files, regardless of their file names.

15. The Gnutella network uses SHA1 values to improve network efficiency. Users may receive a selected file from

numerous sources by accepting segments of the file from multiple peers. The Gnutella software being used then reassembles the complete file on the local computer. The Gnutella program succeeds in reassembling the file from different sources only if all the segments came from the exact copy of the same file. The network uses SHA1 values to ensure exact copies of the same file are used during this process.

16. Upon connecting to the Gnutella network, the Gnutella software being used compiles a list of the shared files, file details and the file's associated SHA1 values. This list is then submitted to the ultra-peers. This information is then propagated to other ultra-peers throughout the network and made available to anyone running a unique search.

17. The frequency of updating information as file changes occur or candidates leave the network depends upon the client software being used and Gnutella networking protocols. The information sent to the ultra-peers is data about the file and not the actual file. The file remains on the peer computer. In this capacity, the ultra-peer acts as a pointer to the files located on each peer.

18. The Gnutella software allows the user to search for pictures, movies, and other files by entering descriptive text as search terms. These terms are typically processed by the ultra-peers based upon the information about the files submitted by the Gnutella user. Entering search terms into a Gnutella client program returns a list of files and descriptive

information pertaining to each file, including the associated SHA1 signature.

19. I know that an investigator is able to compare the SHA1 signatures of files being shared on the network to previously identified child pornography SHA1 signatures.

20. Using a publicly available Gnutella client, an investigator can select the SHA1 signature of a known file as they attempt to locate and download the known file from the Gnutella network.

21. Once a specific file is identified, the download process can be initiated. Once initiated, an investigator is presented with a list of peer or user IP addresses that have been recently (generally within the last 24 hours) identified as candidates for download. This allows for the detection and investigation of computers involved in possessing, receiving and/or distributing files of previously identified child pornography.

22. I know that IP addresses can be used to identify the location of a computer. A computer can be traced to a specific region or area. The ability to identify the location of these IP addresses is provided by IP geographic mapping services, which are publicly available and also used for marketing and fraud detection.

23. A review of the SHA1 signatures allows an investigator to identify the files that are on a peer computer.

24. At this point in the investigative process, a recent (generally within the last 24 hours) association between a known file (based upon SHA1 comparison) and a computer having a specific IP address located within a specific region can be established.

25. Once this association has been established, an investigator can attempt to download a file previously identified as "child notable" from the associated peer. "Child notable" means an image or video that another user of the Child Protection System[2] ("CPS") has viewed and documented as child pornography, with a description in their media library, as part of a criminal investigation.

26. If the function known as browsing is turned on, the investigator can view or browse the contents of the target peer's shared folder. This is dependent upon several factors, including the Gnutella configuration and available resources. Browsing may or may not be possible. If browsing is available, a listing of the files being shared by the associated target

[2] The Child Protection System is a law enforcement tool accessed via the Grid Cop website. Access and a license to CPS is granted to law enforcement personnel after completion of a three-day training course about the use of CPS and ShareazaLE. ShareazaLE is a peer-to-peer client software program developed by the Child Rescue Coalition. It can access, communicate with, and download from multiple peer-to-peer networks, such as Gnutella, eDonkey, and Ares. ShareazaLE is developed so that it downloads files from a single source rather than multiple sources. Law enforcement users of ShareazaLE are granted access and a license for ShareazaLE after completion of a three day training course. CPS communicates suspect information to the users of ShareazaLE for download.

peer may be viewable. In order to obtain this list of files, a direct connection between the computers must occur. This browsing connection is a default setting. Browsing is open to anyone using the publicly available Gnutella software. The file list can only be obtained if the associated target peer is connected to the Gnutella network and the Gnutella software being used is configured for browsing.

27. By receiving either a browsed file list or portions of a download file from a specific IP address, the investigator can conclude that a computer, in this jurisdiction, is running a Gnutella client and is possessing, receiving and/or distributing specific and known visual depictions of child pornography.

28. This investigation of peer-to-peer file sharing networks is a cooperative effort of law enforcement agencies around the country. Many of these agencies are associated with the ICAC Task Force Programs. Many of the officers involved in this effort are using the technology and methods described herein to investigate peer-to-peer networks. This methodology has led to the issuance and execution of search warrants around the country resulting in many seizures of child pornography and arrests for possession and distribution.

VII. INVESTIGATION OF GNUTELLA NETWORK AND SHAREAZA CLIENT SOFTWARE USING IP ADDRESSES AND GUIDS

29. The term Globally Unique Identifier (“GUID”) is defined as a number that is produced by the Windows Operating System (“Windows OS”) or by some Windows applications to

identify a particular component, application, file, database entry, and/or user when the particular component, application, file, database entry, and/or user is created on a device. GUIDs can be created in a number of ways, but usually they are a combination of a few unique settings based on a specific point in time. Based on my training, experience, and knowledge gained from speaking with other knowledgeable officers, agents, and investigators, the GUID of a Gnutella client software program will remain the same even if the user of the Gnutella client software program utilizes a different IP address. This allows law enforcement to track IP addresses across the Internet when a user of a particular Gnutella client software program receives different IP addresses from the ISP, or when different IP addresses are used by one user through accessing a VPN.

30. In the case of Gnutella Network peer-to-peer file sharing technology, a new GUID will be created on a particular computer if the user uninstalls the Gnutella client software program on the device and then reinstalls the Gnutella client software program on the device. Based on my training, experience, and knowledge gained from speaking with other knowledgeable agents, officers, and investigators, generally an upgrade to a newer version of a Gnutella client software program will not change the GUID, but the installation of a newer version of a Gnutella client software program will change the GUID. Additionally, based on my training, experience, and knowledge gained from speaking with other knowledgeable agents,

officers, and investigators, an individual can generate a new GUID when using Shareaza as their Gnutella network client software program, which the suspect of this investigation is using.

31. In this case, the target of the investigation is using Shareaza as the software program to access Gnutella (as described above in paragraph 13. GUIDs for a particular user of Shareaza can differ for various reasons, including the following: (1) the user is uninstalling and reinstalling Shareaza; (2) the user is using Shareaza to generate a new GUID through the settings function of Shareaza; or (3) the user is accessing Gnutella on multiple devices, each of which would have a different GUID. A difference in GUID between two online sessions of Shareaza, then, does not mean that the Shareaza user during these two sessions is different.

VIII. STATEMENT OF PROBABLE CAUSE

A. Online Investigation

32. Between on or about August 02, 2018 and on or about August 14, 2018, SA Timothy Kirkham, from HSI Orange County, Child Exploitation Investigations Group, was conducting an on-line Internet investigation to identify suspects possessing and sharing child pornography. SA Kirkham used a Law Enforcement Peer to Peer (“P2P”) client software program. This P2P client software program allows investigators to download from a single source (rather than multiple sources). This enables the investigator to be sure that the entire file came from a single

target computer. During his investigation SA Kirkham identified a computer using the Internet Protocol Address (IP) 68.5.130.12 (SUSPECT IP ADDRESS) sharing files of possible child pornography.

33. During the online investigation SA Kirkham was able obtain the following user information:

a. Protocol: Gnutella2.

b. Client Software: Shareaza 2.7.10.2.

c. IP Address: 68.5.130.12.

34. On or about August 03, 2018, SA Kirkham downloaded a partial video file from a computer using the SUSPECT IP ADDRESS, approximately eighteen minutes and seventeen seconds in length, entitled “Falkovideo 2013 Pedomom - Pt 1A - She Abuse 8Yo Daughter.wmv.” I have reviewed this video and it depicts a girl that appears to be approximately seven to nine years old having oral copulation performed on her by an adult female. At approximately fourteen minutes into the video the child begins performing oral copulation on the adult female. Throughout the video, sex toys are also inserted vaginally and anally.

35. On or about August 03, 2018, SA Kirkham downloaded a partial video file from a computer using the SUSPECT IP ADDRESS, approximately fifty-eight seconds in length, entitled “Tara 8Yo Full 0001 Pthc Hussyfan Kingpass Liluplanet.avi.” I have reviewed this video and it depicts a naked girl, approximately nine to eleven years old, who is positioned in what is colloquially referred to as the doggy style position on a bed

spreading her buttocks and exposing her vagina and anus. The girl is wearing a mask that is purple and yellow in color. The camera controller moves closer to the girl and then zooms in on her exposed vagina.

36. On or about August 02, 2018, SA Kirkham downloaded a partial video file from a computer using the SUSPECT IP ADDRESS, approximately three minutes and seventeen seconds in length, entitled “Pthc R@Ygold - Better To Eat - Katerina (Brother Sister Incest - 10Yo Boy And 12Yo Girl) - Penetration-Fucking-Torn-Hymen.avi.” I have reviewed this video, which depicts a naked girl approximately ten to twelve years old performing oral copulation on a naked boy approximately nine to eleven years old. The boy and girl then switch positions and she lies on her back while the boy performs oral copulation on her.

B. Identification of Subscriber of SUSPECT IP ADDRESS and SUBJECT PREMISES

37. According to information provided by Cox Communications (the “ISP”), pursuant to a DHS Summons issued on August 17, 2018 – covering the time period during which the SUSPECT IP ADDRESS was used to distribute the child pornography via the Gnutella network - the SUSPECT IP ADDRESS was assigned to subscriber Rick Brandelli at the SUBJECT PREMISES.

38. On or about September 14, 2018, I reviewed a California Department of Motor Vehicles (“DMV”) record for Rick Brandelli, Licence number C0746975. Further investigation revealed Mr. Brandelli has three adult sons, including Daniel

Brandelli, born on September 22, 1986, who is a registered sex offender and has the above listed address in the sex registrant system. Daniel Brandelli also maintains a California driver's license number D5585650, which also has the above address listed as his residence.

39. On September 14, 2018, at approximately 8:50 a.m., I conducted surveillance at the SUBJECT PREMISES. No vehicles were located in the driveway and no movement was seen at the SUBJECT PREMISES.

40. On October 09, 2018, at approximately 4:22 p.m., I witnessed an adult male matching the description of a driver's license photo of a Rick Brandelli collecting the mail and returning the trash dispenser to the side yard.

IX. TRAINING AND EXPERIENCE ON INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN

40. Based on the information above, there is probable cause to believe that someone at the SUBJECT PREMISES possesses child pornography, and also makes it available for distribution. Based on my training and experience, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who view and possess multiple images of child pornography are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children or from fantasies they may have from viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or in other visual media, or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children sometimes possess and maintain “hard copies” of child pornographic material – that is, pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc. When they do, they generally possess these materials in the privacy and security of their home or some other secure location. When individuals who have a sexual interest in children or images of children collect pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and/or videotapes, they often retain these materials for many years.

d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector’s residence, to enable the individual to view the collection, which is valued highly.

e. Individuals who have a sexual interest in children or images of children may correspond with and/or meet others to share information and materials; often retain correspondence from other child pornography distributors/ collectors; conceal such correspondence as they do with their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact with and who share the same interests in child pornography.

f. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

X. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

41. As used herein, the term “digital device” includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and that during the search of a premises it is not always possible to search digital devices for digital data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover “hidden,” erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35′ x 35′ x 10′ rooms to the ceiling. Further, a 500 gigabyte drive could contain as many as approximately 450 full run movies or 450,000 songs.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

g. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions.

For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime. In addition, decryption of devices and data stored thereon is a constantly evolving field, and law enforcement agencies continuously develop or acquire new methods of decryption, even for devices or data that cannot currently be decrypted.

42. As discussed herein, based on my training and experience I believe that digital devices will be found during the search.

a. I know from my training and experience and my review of publicly available materials that several hardware and software manufacturers offer their users the ability to unlock their devices through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint-recognition, face-recognition, iris-recognition, and retina-recognition. Some devices offer a combination of these biometric features and enable the users of such devices to select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple Inc. (“Apple”) offers a feature on some of its phones and laptops called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which on a cell phone is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the phone, and on a laptop is located on the right side of the “Touch Bar” located directly above the keyboard. Fingerprint-recognition features are increasingly common on modern digital devices. For example, for Apple products, all iPhone 5S to iPhone 8 models, as well as iPads (5th generation or later), iPad Pro, iPad Air 2, and iPad mini 3 or later, and MacBook Pro laptops with the Touch Bar are all equipped with Touch ID. Motorola, HTC, LG, and Samsung, among other companies, also produce phones with fingerprint sensors to enable biometric unlock by fingerprint. The fingerprint sensors for these companies have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. To activate the facial-recognition feature, a user must hold the device in front of his or her face. The device's camera analyzes and records data based on the user's facial characteristics. The device is then automatically unlocked if the camera detects a face with characteristics that match those of the registered face. No physical contact by the user with the digital device is necessary for the unlock, but eye contact with the camera is often essential to the proper functioning of these facial-recognition features; thus, a user must have his or her eyes open during the biometric scan (unless the user previously disabled this requirement). Several companies produce digital devices equipped with a facial-recognition-unlock feature, and all work in a similar manner with different degrees of sophistication, e.g., Samsung's Galaxy S8 (released Spring 2017) and Note8 (released Fall 2017), Apple's iPhone X (released Fall 2017). Apple calls its facial-recognition unlock feature "Face ID." The scan and unlock process for Face ID is almost instantaneous, occurring in approximately one second.

d. While not as prolific on digital devices as fingerprint- and facial-recognition features, both iris- and retina-scanning features exist for securing devices/data. The human iris, like a fingerprint, contains complex patterns that are unique and stable. Iris-recognition technology uses mathematical pattern-recognition techniques to map the iris using infrared light. Similarly, retina scanning casts infrared light into a person's eye to map the unique variations of a person's retinal blood vessels. A user can register one or both eyes to be used to unlock a device with these features. To activate the feature, the user holds the device in front of his or her face while the device directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data from the person's eyes. The device is then unlocked if the camera detects the registered eye. Both the Samsung Galaxy S8 and Note 8 (discussed above) have iris-recognition features. In addition, Microsoft has a product called "Windows Hello" that provides users with a suite of biometric features including fingerprint-, facial-, and iris-unlock features. Windows Hello has both a software and hardware component, and multiple companies manufacture compatible hardware, e.g., attachable infrared cameras or fingerprint sensors, to enable the Windows Hello features on older devices.

43. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to

unlock a device than entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents.

44. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features have been enabled. This can occur when a device has been restarted or inactive, or has not been unlocked for a certain period of time. For example, with Apple's biometric unlock features, these circumstances include when: (1) more than 48 hours has passed since the last time the device was unlocked; (2) the device has not been unlocked via Touch ID or Face ID in eight hours and the passcode or password has not been entered in the last six days; (3) the device has been turned off or restarted; (4) the device has received a remote lock command; (5) five unsuccessful attempts to unlock the device via Touch ID or Face ID are made; or (6) the user has activated "SOS" mode by rapidly clicking the right side button five times or pressing and holding both the side button and either volume button. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time. I do not

know the passcodes of the devices likely to be found during the search.

45. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features (such as with Touch ID devices, which can be registered with up to five fingerprints), and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual who is found at the SUBJECT PREMISES and reasonably believed by law enforcement to be a user of the device to unlock the device using biometric features in the same manner as discussed in the following paragraph.

46. For these reasons, if while executing the warrant, law enforcement personnel encounter a digital device that may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel

to, with respect to Daniel Brandelli who is reasonably believed by law enforcement to be a user of a biometric sensor-enabled device that is (a) located at the SUBJECT PREMISES and (b) falls within the scope of the warrant: (1) compel the use of the Daniel Brandelli's thumb- and/or fingerprints on the device(s); and (2) hold the device(s) in front of the face of Daniel Brandelli with his eyes open to activate the facial-, iris-, and/or retina-recognition feature. With respect to fingerprint sensor-enabled devices, although I do not know which of the fingers are authorized to access any given device, I know based on my training and experience that it is common for people to use one of their thumbs or index fingers for fingerprint sensors; and, in any event, all that would result from successive failed attempts is the requirement to use the authorized passcode or password.

47. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

XI. CONCLUSION

48. For all the reasons described above, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251(d)(advertisement of child pornography), 18 U.S.C. § 2252A(a)(2) (receipt and distribution of child pornography), and 18 U.S.C. § 2252A(a)(5)(B) (possession of child pornography), as described in Attachment B to this affidavit, will be found in a search of the SUBJECT PREMISES, which is further described above and in Attachment A of this affidavit.

____
Kevin Leduc
Special Agent
Homeland Security Investigations

Sworn and subscribed before me this ___ day of October, 2018.

____
THE HONORABLE DOUGLAS F. MCCORMICK
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

PREMISES TO BE SEARCHED

The premises to be searched is the property located at 31251 Belford Drive, San Juan Capistrano, California 92675. The SUBJECT PREMISES is located on the southeast side of Belford Dr. The SUBJECT PREMISES is a two-story family residence with an attached three car garage, one white double garage door and one single white garage door both facing northwest. The SUBJECT PREMISES has a light green wood paneling façade with white trim and a gray shingle roof. The front door of the SUBJECT PREMISES is Northwest facing. The numbers “31251” are affixed in black numbers on the white trim of the house facing the street.

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. §§ 2251(d) (advertisement of child pornography), 2252A(a)(2) (receipt and distribution of child pornography), and 2252A(a)(5)(B) (possession of child pornography), namely:

a. Child pornography, as defined in 18 U.S.C. § 2256(8).

b. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that refer to child pornography, as defined in 18 U.S.C. § 2256(8), including documents that refer to the possession, receipt, distribution, transmission, reproduction, viewing, sharing, purchase, or downloading, production, shipment, ordering, requesting, or trading of child pornography, or documents that refer to a transaction of any kind involving child pornography.

c. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, tending to identify persons involved in the possession, receipt, distribution, transmission, reproduction, viewing, sharing, purchase, or downloading, production, shipment, ordering, requesting, or trading of child pornography, or involved in a transaction of any kind involving child pornography, as defined in 18 U.S.C. § 2256(8).

d. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that identify any minor visually depicted while engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

e. Any and all records, documents, programs, applications, materials, or items that are sexually arousing to individuals who are interested in minors, but that are not in and of themselves obscene or that do not necessarily depict minors involved in sexually explicit conduct. Such material is commonly known as “child erotica” and includes written materials dealing with child development, sex education, child pornography, sexual abuse of children, incest, child prostitution, missing children, investigative techniques relating to child exploitation, sexual disorders, pedophilia, nudist publications, diaries, and fantasy writings.

f. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that pertain to peer-to-peer file-sharing software.

g. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that pertain to accounts with any Internet Service Provider.

h. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, regarding ownership and/or possession of 31251 Belford Drive, San Juan Capistrano, CA 92675 (the “SUBJECT PREMISES”).

i. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

j. With respect to any digital device used to facilitate the above-listed violations or containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related

communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the “search team”) will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 120-day period without first obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, “hidden,” or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as “EnCase” and “FTK” (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques, including to search for known images of child pornography.

c. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

6. During the execution of this search warrant, with respect to Daniel Brandelli ("Brandelli") if located at the SUBJECT PREMISES during the execution of the search and who is reasonably believed by law enforcement to be a user of a biometric sensor-enabled device that is located at the SUBJECT PREMISES and falls within the scope of the warrant, the law enforcement personnel are authorized to: (1) depress the thumb- and/or fingerprints of Brandelli onto the fingerprint sensor of the device (only when the device has such a sensor), and direct

which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of the face of Brandelli with his eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device.

7. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.